Information Technology Disaster Recovery and Business Resumption Planning Guidelines

Effective: July 1, 1993

Table of Contents

Introduction

The purpose of disaster recovery/business resumption planning is to assure continuity of computing and telecommunications operations needed to support critical agency functions. The business resumption plan should aim at achieving a systematic and orderly resumption of all agency computing and telecommunications services. The plan should provide for restoring service as soon as possible. Those functions that are most critical to achieving the agency mission must remain in operation during the recovery period.

Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards and procedures.

Scope

These guidelines apply to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

Exemptions

None.

Guidelines

Emergency response/problem escalation procedures prescribe how to respond to two kinds of situation:

- **Disaster events**. Fires, floods, earthquakes, and bombings are examples of disaster events. They often take the form of unforeseen events that cause damage or lengthy disruption or threaten to do so. One can more readily recognize the situation is a disaster during this type of occurrence.
- **Problem**. A disaster may evolve from a problem that disrupts normal operations and then worsens or continues so long that disruption becomes critical.

Disaster recovery/business resumption plans should specify procedures for both situations. Emergency procedures direct the response to disaster events. Escalation procedures direct the response to problems. Both sets of procedures may result in the declaration of a disaster and activation of the recovery plan.

The Recovery Planning Process

There are nine major phases in the recovery planning process:

1. **Project Planning**: Define the project scope, organize the project, and identify the resources needed.
2. **Critical Business Requirements**: Identify the business functions most important to protect, and the means to protect them. Analyze risks, threats, and vulnerabilities.
3. **Recovery Strategies**: Arrange for alternate processing facilities to use during a disaster. Make sure to store copies of computer files, work-in-process, software, and documentation in a safe place.
4. **Emergency Response/Problem Escalation**: Specify exactly how to respond to emergencies and how to tell when a "problem" has become a potential "disaster."
5. **Plan Activation**: Determine procedures for informing the right people, assessing the impact on operations, and starting the recovery efforts.
6. **Recovery Operations**: Develop the specific steps for reducing the risks of an outage and restoring operations should an outage occur.

7. **Training**: Make sure everyone understands the recovery plan and can carry it out efficiently.
8. **Testing**: Make sure the plan works effectively.
9. **Plan Maintenance**: Make changes and additions to keep the plan current.

The disaster recovery/business resumption planning process provides the preparation necessary to design and document the procedures needed to assure continued agency operations following a disaster. Each agency's process should include the following elements:

Project Planning

Get preliminary management commitment.
Get agreement from senior management on the need for disaster recovery/business resumption planning.

Designate a disaster recovery/business resumption manager.
Designate a person to manage the agency's recovery from a disaster. The designated individual must have sufficient knowledge of information management and information technology (IT) within the agency in order to work effectively with IT hardware and software, the data centers, and service providers in reestablishing information processing and telecommunications services after a disaster has occurred.

Organize a disaster recovery/business resumption planning team.
Organize a team that will be responsible for the detailed technical analysis and planning functions needed for a recovery plan.

Identify individuals from management, data processing, telecommunications, business operating units, and consultants to participate in preparing the disaster recovery/business resumption plan.

Audit current recovery preparedness.
Determine what security/disaster recovery/business resumption plans are in place. Identify what planning remains to be done.

Develop the project schedule.
Estimate task durations, identify responsibilities, assign resources, and document the schedule for plan development.

Specify documentation procedures.

Define recovery program overview.

Identify the scope and aim of the disaster recovery/business resumption plan.

Critical Business Requirements

An agency may carry out hundreds of operations that management and staff consider important. Key resources may be unavailable during a disaster. The agency must concentrate its resources on the operations that are most important for public health, safety, and welfare. The aim of a disaster recovery/business resumption plan is to reduce potential losses, not to duplicate a business-as-usual environment.

1. Perform business impact analysis. Establish an understanding of the business organization and service areas of the agency.
2. Identify the business functions to be addressed in accomplishing a business impact analysis.
   - Identify essential business functions. Essential business functions are those functions that must take place in order to support an acceptable level of business continuity for the agency.
   - Develop an understanding of service areas and interdependencies of the essential functions identified.
   - Establish the priorities of senior agency management. Establish the scope of each service area's disaster recovery/business resumption plan and disaster recovery assumptions. There are three major tasks in this procedure:
     - Identify key senior management personnel.
     - Schedule and conduct interviews.
     - Summarize continuity concerns and priorities.
   - Document the operational and financial impact that could result from a disruption or disaster affecting a service area of the agency. There are four tasks in this procedure:
     - Gather operational and financial impact data.
     - Develop outage impact scenarios.
     - Analyze operational impact.
     - Analyze economic impact.
   - Criteria for establishing the criticality of business functions:
     - The key principle involved is that only those functions that must be performed because they are key to the survival of the organization should be listed as a top priority. The priorities of an agency may change as the duration of the service interruption lengthens. For example, a function that can sustain a delay of 3 days may become a top consideration if the interruption lasts a week.
     - The following criteria are suggested for determining the criticality of business functions. There may be others that are of importance to an agency.
       - Maintenance of public health and safety.
       - Income maintenance for citizens.

- Income maintenance for government employees.
- Payments to vendors for goods and services.
- Requirements for compliance or regulation.
- Effect on state government cash flow.
- Criticality Classification.
- Effect on production and delivery of services.
- Volume of activity and recovery costs.
- Effect on public image.
- Inter-system dependency.

The following categorization is suggested as a means for classifying computer application systems used by an agency:

Category/Classification

- Must be processed in normal mode; no degradation is acceptable.
- Only high priority; e.g., high dollar item transactions or critical reports will be processed.
- Processing will be carried out on a "time available" only basis.
- Processing will be suspended, but data collection will continue.
- No processing or data collection will be carried out until normal computer capacity is reestablished.
- Perform threat, risk, and vulnerability analysis.
  - Determine the threats that could debilitate service areas and cause business interruption.
  - There are many natural and man made threats to service areas which could cause business interruption. Potential threats to consider include personnel, physical environment, hardware/software systems, telecommunications, applications, and operations.
  - Threats affecting contingency planning.

    Natural hazards:

    - Earthquake
    - Tornado
    - Flooding
    - Tsunami
    - Landslide
    - Volcanic eruption
    - Lightning
    - Smoke, dirt, dust
    - Sandstorm or blowing dust

- Windstorm
- Snow/ice storm

Accidents:

- Disclosure of confidential information
- Electrical disturbance
- Electrical interruption
- Spill of toxic chemical

Environmental failure:

- Water damage
- Structural failure
- Fire
- Hardware failure
- Liquid leakage
- Operator/user error
- Software error
- Telecommunications interruption

Intentional acts:

- Alteration of data
- Alteration of software
- Computer virus
- Bomb threat
- Disclosure of confidential information
- Employee sabotage
- External sabotage
- Terrorist activity
- Fraud
- Riot/civil disturbance
- Strike
- Theft
- Unauthorized use
- Vandalism

- Determine the probability of occurrence of an identified threat.
  - Many potential threats occur regularly. For regularly occurring threats, historical occurrences and statistical probabilities are maintained by organizations such as the Federal Emergency Management Agency (FEMA), the Federal Communication Commission (FCC), and the US Fire Administration. Statistics on naturally

occurring disasters, burglaries, power outages, fires, and storms are usually available from local, state, or federal agencies.

  - Local threats to the service area, such as hardware failures and unauthorized data access attempts, are usually logged in the organization's problem tracking system or management status reports.
  - Factors affecting threat occurrence rate:
    - Location
    - Facility environment
    - Data sensitivity/criticality
    - Protection and detection features
    - Visibility
    - Proficiency level
    - Security awareness
    - Emergency training
    - Staff morale
    - Local economic conditions
    - Redundancies
    - Availability and use of written operating and security procedures
    - Compliance level (measure of the level of observance or enforcement of security procedures)
    - Past prosecutions

- Determine the vulnerabilities of service areas to potential threats.
  - Vulnerability, the state of being open to abuse or misuse, or subject to indiscriminate use. A weak point or soft spot, a likelihood for error.
  - For many threats, the vulnerability to a business interruption can be mitigated with controls. For example, a vulnerability to fire damage can be mitigated with Halon fire extinguishers and smoke alarms, as well as preventive policies such as the banning of cigarette smoking near flammable materials. Vulnerability considerations include natural disasters, environment, facility housing, access, work scene, and data value.
  - Typical vulnerabilities to consider:
    - System flaws
    - Inadequate audit/security mechanism
    - Power supply
    - Building construction
    - Access control
    - Fire protection
    - Operating procedures
    - Supply and service procedures

    - Emergency procedures
    - Security procedures and security officer
    - Management
    - Personnel
    - Communications architecture
- Estimate the loss potential of a service area, either by quantitative or qualitative means.
  - The impact of an event is the amount of damage it could cause. The frequency of occurrence of that event is the number of times it could happen. If these two are numbers precisely known, the product of the two would be a statement of loss, that is, Loss = Impact X Frequency of Occurrence. Since the exact impact and frequency usually cannot be specified, it is only possible to approximate the loss with an annual loss exposure (ALE). The ALE is the product of estimated impact and estimated frequency of occurrence per year. This method is the quantitative approach to analyzing loss potential.
  - In the qualitative approach, the probability and impact of an event are estimated in orders-of-magnitude, qualitative terms such as low, medium, or high.

Recovery Strategies

Off-site storage of back-up material.

1. Select off-site storage locations.
   - Identify one or more locations off-site for secure storage of copies of data, documentation, and critical supplies.
   - Agencies that purchase computer services from external providers should arrange with the service provider for off-site storage.
2. Determine off-site storage inventory. Identify specific files, programs, documentation, vendor contracts, supplies, etc. (copies of which should be stored and maintained off-site.) Agencies shall include at least one current copy of their disaster recovery/business resumption plan in the off-site storage inventory.
3. Specify off-site inventory procedures. Determine procedures, schedules, and responsibility for maintaining the contents of the off-site storage facility.
4. Alternate processing capability.
   - Identify requirements for recovery facilities.
   - Determine hardware processing capacity, phone service, data communications service, furniture, and space needed in an alternate processing facility.
5. Select recovery facilities.
   - Rank potential recovery alternatives and select one or more.
   - Produce recovery site procedures guide(s).
   - Document information needed to use at each recovery facility.
6. Document overall recovery strategy.

- Document the general strategy the agency will use in the event of a disaster.
  - The recovery strategy is an overview of the recovery process the organization will follow if hit by a disaster. The strategy should address:
    - Recovery requirements for restoration of critical business operations.
    - Any alternate processing facilities employed.
    - Any alternate manual procedures, forms, staffing, and space.
    - Procedures for obtaining resources.
  - Agencies should also develop strategies for addressing each of the following where relevant:
    - Command centers
    - Alternate business operations
    - Alternate data processing
    - Alternate data communications
    - Alternate voice communications
  - Recovery resource acquisition.

Emergency Response/Problem Escalation

Identify potential threats and develop emergency procedures.

Document the action steps to be taken immediately in responding to damaging events or threats of damage or disruption. Inform all agency staff of documented action steps.

1. The purpose of emergency procedures is to:
   - Protect people.
   - Protect property.
   - Reduce outage duration or loss of IT services or assets.
2. Document the emergency response actions the agency must take immediately to:
   - Protect the lives and safety of all personnel.
   - Gain immediate emergency help from fire, police, hospitals.
   - Reduce outage duration or loss of IT services or assets.
   - Inform agency staff who are members of a Disaster Recovery/Business Resumption Management Team that a serious loss or interruption in service has occurred.
   - Set up a focal point for coordinating the recovery program, sending out information, and assembling personnel.
3. Specify problem escalation guidelines.
   - State the steps to follow for escalating unresolved problems to disaster status.
   - The purpose of problem escalation procedures is to define the steps and time allotments leading up to the declaration of a disaster.

Plan Activation

Develop first alert procedures.

1. Prepare general guidelines for initial notification of a potential disaster situation.
2. Develop disaster confirmation procedures.
   - Develop procedures to manage the initial assessment of a disaster or potential disaster situation.
     - Develop procedures for reporting findings to management.
     - Develop procedures for making initial emergency contacts.
     - Develop procedures for possible command center activation.
   - Develop damage assessment procedures.
     - Develop procedures for damage assessment.
     - Develop procedures for examining the effect of the damage on processing of critical operations.
3. Develop notification procedures.
4. Develop procedures for declaring a disaster, for setting up a command center, and for informing the recovery teams, customers, the public, and suppliers.

Recovery Operations

1. Determine plan activation flow.
2. Outline or chart the steps to follow when a disaster situation has occurred or potentially may occur.
3. Define recovery team organization.
4. Determine the teams that make up the recovery organization.
5. Develop team action plans. There may be several recovery teams, each specializing in some area of technical expertise. Disaster Recovery/Business Resumption Team procedures for each team should use a format like the following:

Team Charter or Function: The particular duties and responsibilities of this team in the event of a disaster.

Team Membership and Organization: The structure of the team, job titles of team members, reporting responsibilities.

Team Interfaces: Include detailed explanations of all the actions to be taken by this team prior to a disaster situation so it can function effectively, with the necessary data, personnel and other resources, if a disaster occurs. This section should cover relationships with

vendors, customers, ongoing tasks to ensure readiness of the plan, training requirements, identification of critical resources, data, and personnel.

Action Procedures: This section provides an outline of the tasks to be carried out. It is written with the assumption that team members know how to do their jobs and just need a guide to ensure nothing is omitted during the normal confusion that will occur in the situation.

Procedures should be designed to be flexible in order to permit their use in varying types and degrees of contingency situation.

Procedures should be detailed enough to permit dependency upon them when no other documentation or knowledge is available.

Plan Appendices: The appendices should contain the material and data that will be used in the event of an actual disaster. Include separate appendices on notification of personnel, resource requirements, forms and documentation, and any other subjects that are required. The requirement is based upon the ability of the particular team to access the information during a disaster. If the data may not be otherwise available, it should be included in the appendix to the disaster recovery/business resumption plan.

Training

Design a disaster recovery/business resumption training program.

- Specify the aim, training activities, schedule, and an administrator for disaster recovery/business resumption training.
- Develop specific training activities.
- Develop an instructional plan for each training activity.
- Develop training evaluation tools.
- Develop techniques aimed at answering the following questions:
  - Are trainees able to perform their recovery responsibilities?
  - How can the agency improve training?
  - How can the agency improve its disaster recovery/business resumption plan?

Testing

Testing is the only method to ensure that:

- Recovery procedures are complete and workable.
- Materials and computer files are available and can be used for alternate processing of critical operations and applications.
- Backup copies of software, documentation, and work-in-process records are adequate and current.

- Training of personnel was effective.

Design a recovery plan testing program.

- **Detail:** Specify tests and assign responsibility for overseeing testing. Agencies using external services shall plan, schedule, and conduct their disaster recovery/business resumption plan testing in cooperation with service providers. The cost of establishing the necessary communication link and running a test at a remote back-up facility is high. A full test involving all agency applications may well be impractical due to budget considerations. Agencies should plan to share test time at the service provider's back-up facility ("hot site").
- **Objectives:** Clearly state the purposes for conducting tests of the recovery plan. These will include aims such as the following:
  - A disaster recovery/business resumption plan is complete and workable.
  - Identifying needed revisions to disaster recovery/business resumption plan.
  - Determine the adequacy of disaster recovery/business resumption training.
  - Identifying needed revisions to the training program.
- **Policy/Guidelines:** Set up the policies and guidelines that will apply to testing of the recovery plan. These will cover such items as the following:
  - Committing the agency to a minimum level of testing.
  - Basing the frequency of plan testing on the frequency of changes in the business environment. Agencies must conduct at least one test per year.
- **The testing or validation methodology adopted by an agency will depend on:**
  - Criticality of agency business functions.
  - Cost of executing the test plan.
  - Budget availability.
  - Complexity of information system and components.
  - Reporting requirements.
- **The test report should include:**
  - Date of test.
  - Objectives of test.
  - Description of test.
  - Results.
  - Recommendations.
- **Distribution list for test reports must include:**
  - DIS.
  - Service provider if computer services are obtained from a source external to the agency.
- **User notification.**

  - Define requirements for informing users of planned tests.
  - Before conducting any testing that requires access to client information, inform the owning department. Get permission to test using the client data.
- **Specification of tests.** Formulate a test schedule. For each test, specify the level of the test, the scope or areas to test, and the frequency or target date of the test.
- **Levels of testing:**
  - Level I ⇒ Adequacy of off-site storage of files and documentation. The purpose of the first level is the evaluation of the adequacy of the off-site storage facility and the existing recovery procedures. Primary concentration should be on the off-site files and documentation necessary for efficient system recovery.
  - Level II ⇒ System restoration using off-site files and documentation on the in-house computers.

    The purpose of the second level is to evaluate recovery of the ability to operate. Primary concentration should be on off-site files and documentation of the operating system, as well as management control of the recovery process.
  - Level III ⇒ System and communications restoration using alternate processing facilities, off-site files and documentation.

    The purpose of the third level is to evaluate recovery capability at an alternate site with a reduced staff.
- **Develop plans for specific tests.**
  - Develop test evaluation tools.
  - Develop forms, checklists, and debriefing strategies to check recovery plan tests.

Plan Maintenance

Assign plan maintenance responsibility.

Establish maintenance procedures and schedules. Provide a schedule for regular, systematic review of the content of the disaster recovery/business resumption plan. Define a procedure for making appropriate changes to the plan.

Develop distribution procedures and lists.

- Provide policies and procedures for distributing the recovery plan parts and updates.
- The disaster recovery/business resumption plan may contain sensitive information about the agency's business, communications, and computing operations. Policy and procedures for distribution of the plan should take this into account.

Related Policy and Standards

IT Disaster Recovery and Business Resumption Planning Policy

IT Disaster Recovery and Business Resumption Planning Standards

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.

Definitions

Catastrophic Disaster: A catastrophic disaster is one in which the outage will probably last more than seven days.

Damage - Damage due to a catastrophic disaster is severe and could involve total destruction of the agency facility. Replacement of equipment or significant renovation of the facility may be necessary.

Command Center: The command center is a local, on or off premise area, from which to manage the emergency situation. It is a focal point for coordinating the recovery program, issuing information, and assembling personnel.

Critical Function: Critical functions are those functions an agency must perform to survive. Failure to perform them would result in serious or irreparable harm to the agency. Impact may take the form of increased operating costs, loss of revenue collection, or inability to provide services to clients.

Disaster: Any unplanned circumstance or event that results in an inability to support critical business functions within the current environment.

Disaster Recovery/Business Resumption Plan: A disaster recovery/business resumption plan is a comprehensive statement of actions to be taken in response to a disaster. It includes documented, tested procedures that, if followed, will assure the availability of the critical resources and facilities required to maintain continuity of operations. Sync.: Contingency Plan, Disaster Recovery Plan, Business Continuity Plan.

Major Disaster: A major disaster is one in which the outage will probably last from two to seven days.

Damage - Damage due to a major disaster is more severe than that due to a minor disaster. For example: in a major disaster, key business units could be without telecommunications capability for an extended period. Or the computer room could suffer heavy damage.

Minor Disaster: A minor disaster is one in which the outage will probably last longer than one shift, but less than two days.

Damage - Damage due to a minor disaster is comparatively light. It may consist of minor damage to hardware, software, or electrical equipment from fire, water, chemicals, etc.

Recovery Teams: Recovery teams are manageable units having common recovery requirements. The recovery teams will very likely parallel an existing agency departmental organization.